Trends in Enterprise Mobility …

The need for business agility along with changing employee behaviors will require enterprises to mitigate operational risk associated with mobility

- 1 Billion smart phones and 1.2 Billion Mobile workers by 2014
- Large enterprises expect to triple their smartphone user base by 2015

- 46% of large enterprises supporting personally-owned devices
- Billions of downloads from App Stores; longer term trend for app deployment

Increasing Demand for Enterprise Applications

- 46% of large enterprises supporting personally-owned devices
- Billions of downloads from App Stores; longer term trend for app deployment

Security Requirements Becoming More Complex

- Threats from rogue applications and social engineering expected to double by 2013
- 50% of all apps send device info or personal details
Adapting to the Bring Your Own Device (BYOD) to Work Trend
- Device Management & Security
- Application management

Achieving Data Separation
- Privacy
- Corporate Data protection

Providing secure access to enterprise applications & data
- Secure connectivity
- Identity, Access & Authorization

Developing Secure Mobile Apps
- Vulnerability testing

Designing an Adaptive Security Posture
- Policy Management
- Security Intelligence

Security and Privacy cited as the number one mobile adoption concern
- 2011 IBM Tech Trends Report
Mobile devices are not only computing platforms but also communication devices, hence mobile security is multi-faceted, driven by customers’ operational needs.
Mobile Security Enabled with IBM Solutions

IBM can bring together a broad portfolio of technologies and services to meet the mobile security needs of customers across multiple industries.
Enterprise Use Case Pattern: Security from Devices to Mobile Apps

Secure endpoint device and data

WiFi

Telecom Provider

Internet

Mobile apps

Web sites

Security Gateway

Corporate Intranet & Systems

Develop, test and deliver safe applications

Secure access to enterprise applications and data

© 2011 IBM Corporation
Customer Objective:

Build Secure Mobile Apps to Drive Efficient Business Processes

Develop, deliver and deploy secure mobile applications to streamline business activities while also delivering a rich user experience

Business Need:
- Tools to develop and test secure mobile applications
- A channel for delivering vetted mobile applications to employees, customers and partners
- A light-weight application platform that provides secure runtime for mobile apps

Solution:
Integrate mobile application development and testing tools into a secure mobile application platform that:
- Provides libraries/tools to secure mobile apps & data
- Tailors enterprise policies for mobile use patterns
- Provides integrity in a delivery channel for enterprise apps
- Easily extends client capabilities to verify apps, secure app content, initiate secure connections etc.

Benefits:
- Customers, employees and partners delivered rich user experiences to which they are accustomed
- High value business processes standardized within an app leading to higher productivity
- Security guidelines enforced by tools and application platform
Application Security Solution: WorkLight

**Security by Design**
- Develop secure mobile apps using corporate best practices
- Code Obfuscation

**Protecting Mobile App Data**
- Encrypted local storage for data
- Offline user access
- Challenge response on startup
- App Authenticity Validation
- Enforcement of organizational security policies

**Enforcing Security Compliance**
- Direct Updates
- Integration with User Security Solutions

**App Management**
- Analytics
- Remote Disabling of apps
Application Security Solution: AppScan

Detection of Vulnerabilities before Apps are Delivered and Deployed
- Known vulnerabilities can be addressed in software development and testing
- Code vulnerable to known threat models can be identified in testing
- Security designed in vs. bolted on

Apps vulnerable To Client-side JavaScript vulnerabilities

40%

Applications with issues in 3rd Party JavaScript code

90%
Customer Objective:

**Offer Secure Access to Corporate Resources to Spur Productivity**

Enable mobile employees, partners and customers to be more productive in generating business value by offering secure access to back-end systems.

**Business Need:**
- Make corporate data and services accessible to mobile employees without exposing systems to unauthorized users
- Enable mobile collaboration with partners or customers and ensure those trust relationships are not compromised

**Solution:**
- Deploy mobile identity/access management and network protection solutions that:
  - Offers single sign-on for multiple mobile apps accessing various back-end services
  - Enables policy-based authorization
  - Provides options for securing channels of communication
  - Delivers consistent enterprise network protection from malicious activity and users

**Benefits:**
- Empowered employees contribute to the organization’s responsiveness and agility
- Effective real-time collaboration with partners and customers
- Organization achieves productivity gains
- Realize cost savings by a single infrastructure to safeguard multiple back-end systems
User Security Solution: IBM Web Access Manager for Mobile

Delivers user security by authenticating & authorizing the user along with their device. Supports open standards applicable to mobile such as OAuth.

IBM Access Manager can be used to satisfy complex authentication requirements. A feature called the External Authentication Interface (EAI) is designed to provide flexibility in authentication.

Federated Identity Manager can be incorporated into the solution to provide federated identity management.
Solution: IBM Mobile Connect

Delivers secure connectivity from mobile devices to back-end systems and adapts to a mobile user's unique requirements such as roaming support and cost-based routing.

A high availability intelligent solution providing:

✓ Mobile VPN
✓ SSL VPN
✓ Least cost routing & data optimization
✓ End-to-end encryption
Customer Objective:

**Achieve Control & Oversight to Deliver a Secure User Experience**

Allow employees to focus on executing their functional roles by offloading mobile device security management to the IT organization

**Business Need:**
- Manage employees’ mobile devices to prevent exposure to various security threats.
- At a minimum, provide visibility and oversight when users employ the device for business use.
- Proactively encourage and enforce security best practices

**Solution:**
- Employ a robust mobile device management infrastructure that can:
  - Assure compliance with corporate security guidelines & policies
  - Deliver security updates (i.e. notifications, malware signatures, etc.)
  - Provide facilities for device wipe, lockdown and application management

**Benefits:**
- Engages employees to establish a balance between self help & employer managed services
- Employees’ time directed at generating business value
- Organization reduces operational risk through greater control
- Realize cost savings in utilizing a single infrastructure to deploy successive device security solutions
Device Security Solution: IBM Endpoint Manager For Mobile

Delivers device security by providing visibility of the devices connected to the enterprise, and supports core capabilities such as device lock, selective wipe and jailbreak detection.

A highly-scalable, unified solution across platforms, device types, and IT functions providing:

- Near-instant deployment of new features and analytics reports in to customer’s environments
- A unified systems and security management solution for all enterprise devices
- Platform to extend integrations with Service Desk, CMDB, SIEM, and other information-gathering systems to mobile devices

- Advanced mobile device management capabilities for iOS, Android, Symbian, and Windows Phone
- Unified management approach capable of automatically enabling VPN access based on security compliance
- Security threat detection and automated remediation
- Will be used internally, extending IBM’s existing 500,000 device endpoint management deployment
Customer Objective:
Gain Visibility and Make Informed Mobile Security Decisions

Deliver an adaptive security posture across various mobile security solutions

Business Need:
- Attain a holistic view of an organization’s mobile security model that consists of more than one solution
- Employ security tactics based on the risk profile of the context to mitigate impact on user experience
- Highlight the need for security challenges to increase compliance

Solution:
- Security analytics:
  - Reporting: gaining visibility across all interactions involving enterprise data and services
  - Risk assessments: calculation of risk profiles of each interaction to inform the security approach to employ
  - Threat detection: active monitoring to identify the emergence of known or new threats

Benefits:
- Security model adapted to user’s context prevents degradation of user experience and increased compliance
- Automation of threat responses mitigates risk and improves productivity
Mobile Security Intelligence: QRadar

- Unified collection, aggregation and analysis architecture for application logs, security events, vulnerability data, identity and access mgmt data, configuration files and network flow telemetry
- A common platform for all searching, filtering, rule writing, and reporting functions
- A single user interface for all log management, risk modeling, vulnerability prioritization, incident detection and impact analysis tasks

Achieve Visibility and Enable Adaptive Security Posture

[Diagram showing Internet, Mobile apps, Websites, Corporate Intranet connected to each other]
Customer Use Cases
European Bank Aims to Deliver Secure Mobile Internet Banking

**Customer Objectives**
- Extend secure access to banking applications to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices

**Target Mobile Platforms**
- iOS (iPad/iPhone)
- Android
- Windows Mobile (future)

**IBM Security Solution**
- IBM Security Access Manager authenticates requests made via HTTPS from hybrid mobile applications running on WorkLight platform to back-end services
- A custom certificates-based authentication mechanism implemented to secure back-end banking application

**Business Value**
- Reduce operational complexity and cost with a single, scalable infrastructure to secure access to various back-end services from multiple mobile applications
- Customizability of authentication mechanism empowers the bank to guarantee the security of its customers
- Safeguard trust relationship between the bank and its customers using a safe app platform that encrypts local data and delivers app updates immediately once they are available
IBM Security Solution
- User Security coupled with Application Security
- IBM Access Manager for Mobile serves as a Reverse Proxy and provides Web Access Management (WAM) for WorkLight Server
- WorkLight server interfaces with banking services to deliver the data to authorized mobile users of the bank’s mobile app
- WorkLight shell for the mobile app provides encrypted cache for app data
Health Insurance Provider Offers Secure Mobile Access

Customer Objectives
• Differentiate from competitors by offering customers greater access by supporting mobility
• Reduce overhead of paper-based claims processing and call-center volume

Target Mobile Platforms
• iOS (iPad/iPhone)
• Android

IBM Security Solution
• Requests made via HTTPS to multiple back-end services from native device applications protected by IBM Security Access Manager
• Authentication enforced with both Basic Authentication and a custom implementation through Access Manager’s External Authentication Interface

Business Value
• Simultaneously build trust and improve user experience with secure membership management and claims processing
• Improve customer satisfaction and responsiveness through secure mobile solutions
Retailer Intends to Protect Corporate Data on Mobile Devices

**Customer Objectives**
- Prevent the loss or leakage of intellectual property and proprietary information
- Deliver tools to defend employees’ mobile devices from malware

**Target Mobile Platforms**
- iOS (iPad/iPhone)
- Android

**IBM Security Solution**
- Remote management of data and applications on mobile devices that includes selective device wipe feature
- Partnerships to deliver anti-malware services

**Business Value**
- Empower employees to collaborate using mobile devices to drive business value while mitigating the risk of data loss
- Govern corporate data and applications and reduce capital expense in acquiring mobile devices
Legal Disclaimer

- © IBM Corporation 2011. All Rights Reserved.
- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- If the text contains performance statistics or references to benchmarks, insert the following language; otherwise delete:
  Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
- If the text includes any customer examples, please confirm we have prior written approval from such customer and insert the following language; otherwise delete:
  All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.
- Please review text for proper trademark attribution of IBM products. At first use, each product name must be the full name and include appropriate trademark symbols (e.g., IBM Lotus® Sametime® Unyte™). Subsequent references can drop “IBM” but should include the proper branding (e.g., Lotus Sametime Gateway, or WebSphere Application Server). Please refer to http://www.ibm.com/legal/copytrade.shtml for guidance on which trademarks require the ® or ™ symbol. Do not use abbreviations for IBM product names in your presentation. All product names must be used as adjectives rather than nouns. Please list all of the trademarks that you use in your presentation as follows; delete any not included in your presentation. IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.
- If you reference Adobe® in the text, please mark the first use and include the following; otherwise delete:
  Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- If you reference Java™ in the text, please mark the first use and include the following; otherwise delete:
  Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- If you reference Microsoft and/or Windows® in the text, please mark the first use and include the following, as applicable; otherwise delete:
  Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- If you reference Intel® and/or any of the following Intel products in the text, please mark the first use and include those that you use as follows; otherwise delete:
  Intel, Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- If you reference UNIX® in the text, please mark the first use and include the following; otherwise delete:
  UNIX is a registered trademark of The Open Group in the United States and other countries.
- If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:
  Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.
- If the text/graphics include screenshots, no actual IBM employee names may be used (even your own), if your screenshots include fictitious company names (e.g., Renovations, Zeta Bank, Acme) please update and insert the following; otherwise delete: All references to [insert fictitious company name] refer to a fictitious company and are used for illustration purposes only.